

信息处理

技术领域

[01]本说明书一个或多个实施例涉及计算机应用技术领域，尤其涉及信息处理方法和装置。

背景技术

[02]随着计算机和互联网技术的迅速发展，为人类生产和生活带来了越来越多的便利。诸如条形码、二维码等信息码技术作为近几年来移动设备上流行的一种编码方式，也给诸如支付、打卡、信息获取等应用场景带来了极大便利。例如，对于金融类应用，常常在其中嵌入本金融机构的支付码，当用户打开该支付码后可供给商家扫描以完成支付。然而，基于安全性的考虑，目前诸如支付码之类的信息码往往只能在本金融机构的客户端内使用，这就造成用户需要在终端设备上安装各种金融类应用的客户端，从而造成了资源的占用和使用的不便。

发明内容

[03]本说明书一个或多个实施例描述了一种信息处理方法和装置，以便于提高信息码的使用便利性，降低对终端设备资源的占用。

[04]根据第一方面，提供了一种信息处理方法，由信息码服务器端执行，包括：接收来自第二客户端的信息码处理请求，所述信息码处理请求由所述第二客户端扫描第一客户端嵌入的第三方信息码后发送；依据所述信息码处理请求进行风险识别；依据识别得到的风险信息和预设的安全规则，执行相应的处理逻辑；向所述第一客户端发送所述处理逻辑的处理结果。

[05]在一个实施例中，所述依据所述信息码处理请求进行风险识别包括：依据所述信息码处理请求携带的交易信息、设备信息、环境信息和时间信息中的至少一种，识别得到风险信息；或者，依据所述信息码处理请求携带的用户信息查询所述用户的历史数据，依据所述用户的历史数据识别得到风险信息。

[06]在另一个实施例中，所述依据识别得到的风险信息和预设的安全规则，执行相应的处理逻辑包括：依据识别得到的风险信息查询预设的安全规则，确定是否执行安全校验；如果是，执行与所述风险信息对应的安全校验后，执行所述信息码对应的处理逻辑；否则，执行信息码对应的处理逻辑。

[07]在一个实施例中，所述安全校验包括：用户确认、密码校验、数字证书校验、密码结合数字证书校验或者跳转至第三方信息码对应的客户端。

[08]在另一个实施例中，所述密码校验包括：依据所述信息码处理请求携带的用户信息，确定用户最新设置的密码类型信息和第一密码信息；向所述第一客户端发送包含所述密

码类型信息的密码校验消息；获取所述第一客户端发送的第二密码信息，利用所述第二密码信息和第一密码信息进行校验。

[09]在一个实施例中，所述数字证书校验包括：依据所述信息码处理请求携带的用户信息，确定与所述用户信息对应的第一数字证书信息；向所述第一客户端发送校验数字证书的消息；获取所述第一客户端发送的第二数字证书信息，利用所述第二数字证书信息和所述第一数字证书信息进行校验。

[10]在另一个实施例中，所述密码结合数字证书校验包括：依据所述信息码处理请求携带的用户信息，确定与所述用户信息对应的密码类型信息、第一密码信息和第一数字证书信息；向所述第一客户端发送校验密码和数字证书的消息；获取所述第一客户端发送的第二密码信息和第二数字证书信息，利用第一密码信息、第二密码信息、第一数字证书信息和第二数字证书信息进行校验。

[11]在一个实施例中，所述信息码包括支付码，所述处理逻辑包括支付处理。

[12]根据第二方面，提供了一种信息处理方法，由第一客户端执行，包括：响应于打开第三方信息码的触发事件，展现包含第三方信息码的界面，以便于第二客户端扫描所述第三方信息码并触发所述第三方信息码的处理逻辑；获取到信息码服务器端发送的所述处理逻辑的处理结果后，展现包含所述处理结果的界面。

[13]在一个实施例中，所述打开第三方信息码的触发事件包括：用户触发所述第一客户端中打开第三方信息码的组件；或者，用户在锁屏界面上执行的预设手势操作。

[14]在另一个实施例中，该方法还包括：接收到所述信息码服务器端发送的包含密码类型信息的密码校验消息后，展示输入所述类型密码的提示界面，将用户输入的第二密码信息发送给所述信息码服务器端；或者，接收到所述信息码服务器端发送的校验数字证书的消息后，向所述信息码服务器端发送第二数字证书信息；或者，接收到所述信息码服务器端发送的校验密码和数字证书的消息后，该消息包含密码类型信息，展示输入所述类型密码的提示界面，并将第二数字证书信息以及用户输入的第二密码信息发送给信息码服务器端。

[15]根据第三方面，提供了一种信息处理装置，设置于信息码服务器端，该装置包括：接收单元，被配置为接收来自第二客户端的信息码处理请求，所述信息码处理请求由所述第二客户端扫描第一客户端嵌入的第三方信息码后发送；识别单元，被配置为依据所述信息码处理请求进行风险识别；执行单元，被配置为依据识别得到的风险信息和预设的安全规则，执行相应的处理逻辑；发送单元，被配置为向所述第一客户端发送所述处理逻辑的处理结果。

[16]在一个实施例中，所述识别单元，具体被配置为：依据所述信息码处理请求携带的交易信息、设备信息、环境信息和时间信息中的至少一种，识别得到风险信息；或者，

依据所述信息码处理请求携带的用户信息查询所述用户的历史数据，依据所述用户的历史数据识别得到风险信息。

[17]在另一个实施例中，所述执行单元包括：确认子单元，被配置为依据识别得到的风险信息查询预设的安全规则，确定是否执行安全校验；校验子单元，被配置为若所述确认子单元确定执行安全校验，则执行与所述风险信息对应的安全校验；执行子单元，被配置为若通过安全校验，则执行所述信息码对应的处理逻辑；若所述确认子单元确定不执行安全校验，则执行所述信息码对应的处理逻辑。

[18]在一个实施例中，所述安全校验包括：用户确认、密码校验、数字证书校验、密码结合数字证书校验或者跳转至第三方信息码对应的客户端。

[19]在另一个实施例中，所述校验子单元在执行密码校验时，具体被配置为：依据所述信息码处理请求携带的用户信息，确定用户最新设置的密码类型信息和第一密码信息；向所述第一客户端发送包含所述密码类型信息的密码校验消息；获取所述第一客户端发送的第二密码信息，利用所述第二密码信息和第一密码信息进行校验。

[20]在一个实施例中，所述校验子单元在执行数字证书校验时，具体被配置为：依据所述信息码处理请求携带的用户信息，确定与所述用户信息对应的第一数字证书信息；向所述第一客户端发送校验数字证书的消息；获取所述第一客户端发送的第二数字证书信息，利用所述第二数字证书信息和所述第一数字证书信息进行校验。

[21]在另一个实施例中，所述校验子单元在执行密码结合数字证书校验时，具体被配置为：依据所述信息码处理请求携带的用户信息，确定与所述用户信息对应的密码类型信息、第一密码信息和第一数字证书信息；向所述第一客户端发送校验密码和数字证书的消息；获取所述第一客户端发送的第二密码信息和第二数字证书信息，利用第一密码信息、第二密码信息、第一数字证书信息和第二数字证书信息进行校验。

[22]在一个实施例中，所述信息码包括支付码，所述处理逻辑包括支付处理。

[23]根据第四方面，提供了一种信息处理装置，设置于第一客户端，该装置包括：展现单元，被配置为响应于打开第三方信息码的触发事件，展现包含第三方信息码的界面，以便于第二客户端扫描所述第三方信息码并触发所述第三方信息码的处理逻辑；交互单元，被配置为获取信息码服务器端发送的所述处理逻辑的处理结果；所述展现单元，还被配置为展现包含所述处理结果的界面。

[24]在一个实施例中，所述打开第三方信息码的触发事件包括：用户触发所述第一客户端中打开第三方信息码的组件；或者，用户在锁屏界面上执行的预设手势操作。

[25]在一个实施例中，所述交互单元进一步被配置为：接收所述信息码服务器端发送的包含密码类型信息的密码校验消息，将用户输入的第二密码信息发送给所述信息码服务器端；或者接收所述信息码服务器端发送的校验数字证书的消息，向所述信息码服务器

端发送第二数字证书信息；或者，接收所述信息码服务器端发送的校验密码和数字证书的消息，向所述信息码服务器端发送第二数字证书信息；所述展现单元进一步被配置为：展示输入所述类型密码的提示界面。

[26]根据第五方面，提供了一种计算设备，包括存储器和处理器，所述存储器中存储有可执行代码，所述处理器执行所述可执行代码时，实现第一方面的方法。

[27]根据本说明书实施例提供的方法和装置，在第一客户端中嵌入第三方信息码，从而使得用户无需逐一安装各信息码的客户端，从而降低对终端设备资源的占用，提高信息码的使用便利性。

[28]并且，在信息码服务器端，通过风险识别和安全规则保证了信息码对应处理逻辑的安全性。

附图说明

[29]为了更清楚地说明本发明实施例或现有技术中的技术方案，下面将对实施例或现有技术描述中所需要使用的附图作简单地介绍，显而易见地，下面描述中的附图是本发明的一些实施例，对于本领域普通技术人员来讲，在不付出创造性劳动的前提下，还可以根据这些附图获得其他的附图。

[30]图 1 示出了根据一个实施例的信息处理方法的流程图；

[31]图 2a 示出了根据一个实施例的第三方支付码的嵌入方式示意图；

[32]图 2b 示出了根据一个实施例的从包含支付码的界面跳转至包含支付成功信息的界面的示意图；

[33]图 2c 示出了根据一个实施例的以通知消息的方式展现处理结果的界面示意图；

[34]图 3 示出了根据一个实施例的信息处理方法的流程图；

[35]图 4 示出了根据一个实施例的在支付流程中采用用户确认方式的流程图；

[36]图 5 示出了根据一个实施例的在支付流程中采用密码校验方式的流程图；

[37]图 6 示出了根据一个实施例的在支付流程中采用数字证书校验方式的流程图；

[38]图 7 示出了根据一个实施例的在支付流程中采用密码结合数字证书校验方式的流程图；

[39]图 8 出了根据一个实施例的在支付流程中采用跳转至第三方信息码客户端的流程图；

[40]图 9 示出了根据一个实施例的信息处理装置的示意性框图；

[41]图 10 示出根据另一个实施例的信息处理装置的示意性框图。

具体实施方式

[42]下面结合附图，对本说明书提供的方案进行描述。

[43]本说明书的核心思路在于，在客户端中能够嵌入各第三方信息码，从而使得用户无

需逐一安装各信息码的客户端，从而降低对终端设备资源的占用，提高信息码的使用便利性。

[44]下面描述以上构思的具体实现方式。

[45]图 1 示出了根据一个实施例的信息处理方法的流程图。该方法由第一客户端执行。该第一客户端嵌入有第三方信息码。如图 1 所示，该方法包括以下步骤。

[46]步骤 101，响应于打开第三方信息码的触发事件，第一客户端展现包含第三方信息码的界面，以便于第二客户端扫描该第三方信息码并触发第三方信息码的处理逻辑。

[47]步骤 103，第一客户端获取到上述处理逻辑的处理结果后，展现包含该处理结果的界面。

[48]下面描述图 1 所示的各个步骤的执行方式。本发明实施例提供的技术方案中，信息码可以是诸如条形码、二维码等能够承载编码信息的图形，在公开后续实施例中均以二维码为例进行描述。另外，信息码可以用以进行支付、转账、签到、提供身份信息等功能，在后续实施例中均以作为支付码用以完成支付功能为例。

[49]首先对步骤 101 即“响应于打开第三方信息码的触发事件，第一客户端展现包含第三方信息码的界面，以便于第二客户端扫描该第三方信息码并触发第三方信息码的处理逻辑”进行详细描述。

[50]其中，打开第三方信息码的触发事件可以包括但不限于以下两种方式。

[51]第一种方式，用户触发第一客户端中打开第三方信息码的组件。

[52]在第一客户端中嵌入第三方信息码时，通常第三方信息码的链接会以组件的形式在第一客户端中展现。如图 2a 中所示，第一客户端可以是“钱包”客户端，第三方支付码可以是以卡片的形式嵌入“钱包”客户端。当用户点击该卡片后，展现该第三方支付码。

[53]第二种方式，用户在锁屏界面上执行的预设手势操作。

[54]为了更加快捷地打开第三方信息码，第一客户端可以通过设置锁屏界面的快捷手势作为预设手势操作，例如在锁屏界面上双击屏幕。当用户在锁屏界面双击屏幕后，第一客户端展现第三方信息码给用户。

[55]除了上述方式之外，还可以采用其他事件作为打开第三方信息码的触发事件，例如在第一客户端中通过语音方式调出包含第三方信息码的界面。

[56]上述第二客户端可以是用以从第三方信息码中获取信息的客户端。例如商家的客户端扫描用户“钱包”客户端中嵌入的第三方支付码，从而实现对商家所提供商品或服务的支付功能。再例如，公司的客户端扫描员工客户端中嵌入的第三方签到码，从而实现员工在公司的签到功能。

[57]通常第二客户端触发第三方信息码的处理逻辑，是通过向第三方信息码的服务器（本说明书中称其为“信息码服务器”）发送处理请求来实现的，由信息码服务器完成相应的

处理逻辑，并向第一客户端发送处理结果。除此之外，信息码服务器还可以向第二客户端返回处理结果。

[58]例如第二客户端向信息码服务器发送码支付请求，信息码服务器完成支付流程后，向第一客户端和第二客户端发送支付处理结果。

[59]下面对步骤 103 即“第一客户端获取到上述处理逻辑的处理结果后，展现包含该处理结果的界面”进行详细描述。

[60]信息码服务器向第一客户端发送处理结果后，第一客户端可以采用但不限于以下方式展现包含处理结果的界面。

[61]第一种方式：从当前界面跳转至包含上述处理逻辑的处理结果的界面。其中，处理结果可以包括是否处理成功的信息，还可以包括其他与处理逻辑相关的信息。

[62]如图 2b 中所示，从包含支付码的界面跳转至包含支付成功信息的界面，该界面中除了包含支付成功的信息之外，还可以包括支付金额、交易相关信息等。

[63]第二种方式：以通知消息的方式展现包含上述处理逻辑的处理结果的界面。

[64]如图 2c 中所示，在界面显示通知消息。图 2c 中以从屏幕顶部显示通知消息为例，但并不限于这种通知消息的显示位置和形式。当用户点击该通知消息时，展现包含支付成功的信息。该界面中除了包含支付成功的信息之外，还可以包括支付金额、交易相关信息等。

[65]本发明所涉及的展现操作，可以包括但不限于渲染操作与显示操作中至少一项操作，本实施例对此不进行特别限定。具体地，执行主体所展现的内容，就是渲染操作所输出的渲染结果，渲染操作可以由网络侧服务器中的渲染引擎根据目标页面的页面源代码执行，进而将渲染结果以位图图像形式，或者矢量图像等其他形式，进行存储处理，并提供给执行主体输出所述渲染结果，或者还可以由执行主体根据目标页面的页面源代码执行，进而直接输出渲染结果。

[66]图 3 示出了根据一个实施例的信息处理方法的流程图。该方法由信息码服务器端执行，信息码服务器端可以是一个服务器，也可以是多个服务器构成的服务器集群。如图 3 所示，该方法可以包括以下步骤。

[67]步骤 301：接收来自第二客户端的信息码处理请求，信息码处理请求由第二客户端扫描第一客户端嵌入的第三方信息码后发送。

[68]步骤 303：依据信息码处理请求进行风险识别。

[69]步骤 305：依据识别得到的风险信息和预设的安全规则，执行相应的处理逻辑。

[70]步骤 307：向第一客户端发送上述处理逻辑的处理结果。

[71]由于一些信息码诸如支付码等，对于安全性有着极高的要求。作为其中一种可实现的方式，可以通过向第一客户端提供 SDK (Software Development Kit, 软件开发工具包)

的方式实现第一客户端的相关功能。但这种方式需要第一客户端集成第三方 SDK。

[72]作为其中一种优选的实施方式，并不向第一客户端提供 SKD，由第一客户端自己的代码来实现，那么就需要依靠图 3 所示实施例中风险识别和安全规则来保证处理逻辑的安全性。

[73]下面描述图 3 所示的各个步骤的执行方式。首先对步骤 303 即“依据信息码处理请求进行风险识别”进行详细描述。

[74]作为其中一种可实现的方式，可以依据信息码处理请求携带的交易信息、设备信息和环境信息中的至少一种，识别得到风险信息。

[75]以支付码场景为例，上述交易信息可以包括商家信息、交易金额、支付渠道信息等。例如可以依据其中的交易金额，当交易金额超过预设的不同阈值时，认为存在相应的风险。例如可以依据其中的商家信息、交易金额等多种信息判定当前交易为欺诈时，认为存在相应的风险。

[76]上述设备信息可以是用户所使用的设备类型、设备标识等等。例如用户使用的是常用设备，则认为具有较低风险或者没有风险。若用户使用的并非常用设备，则认为具有一定风险。

[77]上述环境信息可以是用户所处的网络类型、网络标识等等。例如用户使用的是常用的局域网，则认为风险较低。若用户使用的并非常用局域网，则认为具有一定风险。

[78]上述时间信息可以是在第二客户端扫描信息码时的时间信息，发送信息码请求的时间信息等等。例如，如果第二客户端扫描信息码的时间信息与展示信息码的时间信息之间的差值超出预设的时长阈值，则认为具有一定风险。

[79]作为另一种可实现的方式，可以依据信息码处理请求携带的用户信息查询用户的历史数据，依据用户的历史数据识别得到风险信息。

[80]用户的历史数据可以包括诸如是否修改过密码、用户历史交易行为是否存在异常等等。

[81]对于上述风险信息，可以采用风险场景信息来表示。例如风险信息表示为“用户修改过密码”、“支付金额大于 X 且用户具有可用数字证书”、“支付金额大于当前支付渠道可用余额”、“非用户常用设备”、“非常用网络环境”等等。

[82]上述风险信息也可以采用风险等级来表示，例如划分为高、中、低风险。再例如划分为一级风险、二级风险、三级风险、四级风险等等。

[83]下面对步骤 305 即“依据识别得到的风险信息和预设的安全规则，执行相应的处理逻辑”进行详细描述。

[84]在本步骤中涉及的处理逻辑可以一方面包含安全校验的部分，另一方面包含信息码本身的处理逻辑。其中安全校验可以依据风险识别得到的风险信息来确定是否进行以及

进行怎样的安全校验。

[85]作为其中一种实现方式，可以首先依据识别得到的风险信息查询预设的安全规则，确定是否执行安全校验；如果是，执行与风险信息对应的安全校验后，执行信息码对应的处理逻辑；否则，执行信息码对应的处理逻辑。

[86]其中，上述执行的安全校验可以包括：用户确认、密码校验、数字证书校验、密码结合数字证书校验或者跳转至第三方信息码对应的客户端。

[87]上述安全规则的内容实际上包含的是风险信息与安全校验之间的对应关系。例如：信息码被扫描的时间与展示时间之间的差值超过预设时长阈值，例如支付码超过1分钟才被请求支付，则可以采用用户确认的安全校验方式。

[88]用户密码被修改，其中密码可以包括PIN密码，也可以包括诸如指纹、人脸、虹膜等生物特征密码，则可以采用密码校验的安全校验方式。

[89]用户历史交易行为存在异常，则可以采用密码校验的安全校验方式。

[90]支付金额超过X元且用户不具有可用数字证书，则采用证书验证的方式。

[91]支付金额超过Y元且用户有可用数字证书，则采用证书验证的方式。

[92]其中，上述的X和Y为预设金额阈值。

[93]支付金额大于当前支付渠道可用余额，则采用跳转至第三方信息码对应的客户端的方式。

[94]支付金额超过预设的支付限额，则采用跳转至第三方信息码对应的客户端的方式。

[95]当前交易被判定为欺诈，则采用跳转至第三方信息码对应的客户端的方式。

[96]上述安全规则仅仅为列举的实例，在此无法对所有安全规则进行一一列举。在此精神原则之内的替换、转换或类似延伸均在本发明所保护的范围内。

[97]下面对上述几种安全校验的方式进行描述：用户确认可以包括：向第一客户端发送确认本次处理逻辑的消息，在预设时长内接收到第一客户端返回的包含用户确认信息的请求后，认为本次校验通过。如果超过预设时长未接收到第一客户端返回的包含用户确认信息的请求，或者，接收到第一客户端返回的包含用户未确认信息的请求，则认为本次校验失败。

[98]这种校验方式下，第一客户端接收到包含用户确认信息的请求后，展现用户输入确认信息的提示界面；获取到用户输入的确认信息或未确认信息后，发送给信息码服务器端。

[99]密码校验可以包括：依据信息码处理请求携带的用户信息，确定用户最新设置的密码类型信息和第一密码信息。向第一客户端发送包含密码类型信息的密码校验消息；获取第一客户端发送的第二密码信息，利用第二密码信息和第一密码信息进行校验。如果第一密码信息和第二密码信息一致，则认为本次校验通过，否则认为本次校验失败。

[100]这种校验方式下,第一客户端接收信息码服务器端发送的包含密码类型信息的密码校验消息后,展示输入对应类型密码的提示界面,并将用户输入的第二密码信息发送给信息码服务器端。

[101]数字证书校验可以包括:依据信息码处理请求携带的用户信息,确定与用户信息对应的第一数字证书信息;向第一客户端发送校验数字证书的消息;获取第一客户端发送的第二数字证书信息,利用第二数字证书信息和第一数字证书信息进行校验。如果第一数字证书信息和第二数字证书信息一致,则认为本次校验通过,否则认为本次校验失败。其中,第一数字证书信息可以是服务器端的签名信息,第二数字信息可以是客户端的签名信息。

[102]这种校验方式下,第一客户端接收到信息码服务器端发送的校验数字证书的消息后,向信息码服务器端发送第二数字证书信息。

[103]密码结合数字证书校验可以包括:依据信息码处理请求携带的用户信息,确定用户最新设置的密码类型信息、第一密码信息和用户信息对应的第一数字证书信息;向第一客户端发送校验密码和数字证书的消息;获取第一客户端发送的第二密码信息和第二数字证书信息,利用第一密码信息、第二密码信息、第一数字证书信息和第二数字证书信息进行校验。

[104]这种校验方式下,第一客户端接收到信息码服务器端发送的校验密码和数字证书的消息后,展示输入对应类型密码的提示界面,并将第二数字证书信息以及用户输入的第二密码信息发送给信息码服务器端。

[105]跳转至第三方信息码对应的客户端包括:向第一客户端发送指示跳转至第三方信息码对应客户端的链接,该链接中包含信息码对应的处理逻辑信息,例如支付码对应的相关支付信息。第一客户端接收到该链接后跳转至第三方信息码对应客户端,由第三方信息码对应的客户端与信息码服务器进行交互以完成后续处理逻辑。

[106]下面以支付码对应的支付流程为例,结合具体实施例对上述几种校验方式进行详细描述。

[107]图4示出了根据一个实施例的在支付流程中采用用户确认方式的流程图,如图4中所示,该流程可以包括以下步骤。

[108]步骤401:第二客户端扫描第一客户端的第三方信息码。

[109]步骤403:第二客户端向信息码服务器端的验证执行模块发送码支付请求。

[110]步骤405:验证执行模块向安全模块进行风险咨询。

[111]步骤407:安全模块向存储模块发送安全规则 and 用户历史数据的查询。

[112]步骤409:存储模块将安全规则 and 用户历史数据发送给安全模块。

[113]步骤411:安全模块进行风险识别,确定采用的校验方式。本流程中确定采用用户

确认方式。

[114]步骤 413: 安全模块将用户确认方式的信息通知给验证执行模块。

[115]步骤 415: 验证执行模块向第一客户端发送要求用户确认支付信息的信息。

[116]第一客户端接收到该消息后, 会向用户展现要求用户确认支付信息的界面, 用户可以在该界面上选择确认或不确认。

[117]步骤 417: 验证执行模块获取到包含用户确认支付信息的支付请求后, 触发支付逻辑。

[118]其中触发支付逻辑实际上就是与支付服务器进行交互, 以完成用户支付的处理, 例如支付服务器从用户账户中扣除相应支付金额, 用以付款给商家。该部分支付逻辑可以采用已有的交互处理流程, 在此不做详述。

[119]上述流程中关于发送码支付请求、风险识别、确定校验方式等的具体处理方式可以参见上面方法实施例中的相关记载, 在此流程中不做赘述。

[120]另外, 在上述实施例所示流程以及后续实施例所示流程中, 验证执行模块、安全模块和存储模块可以设置于同一服务器, 也可以分别设置于不同的服务器。这些模块之间可以经由其他模块进行信息的转发, 这些其他模块在图中并未示出。第一客户端和验证执行模块之间以及第二客户端和验证执行模块之间可以通过诸如路由设备、接入设备、第一客户端或第二客户端对应的转发设备等网络设备进行信息的转发, 这些设备在图中并未示出。

[121]图 5 示出了根据一个实施例的在支付流程中采用密码校验方式的流程图, 如图 5 中所示, 该流程可以包括以下步骤。

[122]步骤 501: 第二客户端扫描第一客户端的第三方信息码。

[123]步骤 503: 第二客户端向信息码服务器端的验证执行模块发送码支付请求。

[124]步骤 505: 验证执行模块向安全模块进行风险咨询。

[125]步骤 507: 安全模块向存储模块发送安全规则和用户历史数据的查询。

[126]步骤 509: 存储模块将安全规则和用户历史数据发送给安全模块。

[127]步骤 511: 安全模块进行风险识别, 确定采用的校验方式。本流程中确定采用密码校验方式。

[128]例如用户历史数据表明用户更改了密码, 则该用户历史数据中包含用户最新的第一密码信息。

[129]步骤 513: 安全模块将采用密码校验方式的信息和用户的第一密码信息发送给验证执行模块。

[130]步骤 515: 验证执行模块从第一密码信息中提取密码类型信息。

[131]即从第一密码信息中获取用户最新采用的密码类型是什么, 例如指纹信息、人脸信

息、PIN 密码等。

[132]步骤 517: 验证执行模块向第一客户端发送包含密码类型信息的密码校验消息。

[133]第一客户端接收到该密码校验消息后, 会向用户展现要求用户输入上述类型密码的界面。例如要求用户输入指纹、人脸、PIN 密码等作为第二密码信息。

[134]步骤 519: 第一客户端将用户依据密码类型信息输入的第二密码信息发送给验证执行模块。

[135]步骤 521: 验证执行模块利用第一密码信息和第二密码信息进行密码校验。

[136]步骤 523: 校验成功后, 触发支付逻辑。

[137]更进一步地, 在密码校验之后, 还可以进一步向存储模块发送密码变更后本次密码校验的信息, 这部分作为新的用户历史数据记录于存储模块。

[138]图 6 示出了根据一个实施例的在支付流程中采用数字证书校验方式的流程图, 如图 6 中所示, 该流程可以包括以下步骤。

[139]步骤 601: 第二客户端扫描第一客户端的第三方信息码。

[140]步骤 603: 第二客户端向信息码服务器端的验证执行模块发送码支付请求。

[141]步骤 605: 验证执行模块向安全模块进行风险咨询。

[142]步骤 607: 安全模块向存储模块发送安全规则 and 用户历史数据的查询。

[143]步骤 609: 存储模块将安全规则 and 用户历史数据发送给安全模块。

[144]步骤 611: 安全模块进行风险识别, 确定采用的校验方式。本流程中确定采用数字证书校验方式。

[145]例如用户历史数据表明该用户安装有数字证书且支付金额超过 X 元, 因此确定需要采用数字证书校验方式。

[146]步骤 613: 安全模块向存储模块请求数字证书信息。

[147]步骤 615: 存储模块依据用户标识等提取该用户的第一数字证书信息, 并发送给安全模块。

[148]步骤 617: 安全模块将采用数字证书校验方式的信息和第一数字证书信息发送给验证执行模块。

[149]步骤 619: 验证执行模块向第一客户端发送数字证书校验消息。

[150]步骤 621: 第一客户端获取本地的第二数字证书信息, 并发送给验证执行模块。

[151]第一客户端接收到数字证书校验消息后, 调用本地已安装的数字证书的信息作为第二数字证书信息。

[152]步骤 623: 验证执行模块利用第一数字证书信息和第二数字证书信息进行校验。

[153]步骤 625: 校验成功后, 触发支付逻辑。

[154]另外, 在上述验证过程中, 如果确定采用数字证书校验方式但客户端并未安装数字

证书,则可以触发第二客户端安装数字证书以作为校验方式,在第二客户端安装数字证书后,触发支付逻辑。

[155]图 7 示出了根据一个实施例的在支付流程中采用密码结合数字证书校验方式的流程图,如图 7 中所示,该流程可以包括以下步骤。

[156]步骤 701: 第二客户端扫描第一客户端的第三方信息码。

[157]步骤 703: 第二客户端向信息码服务器端的验证执行模块发送码支付请求。

[158]步骤 705: 验证执行模块向安全模块进行风险咨询。

[159]步骤 707: 安全模块向存储模块发送安全规则和用户历史数据的查询。

[160]步骤 709: 存储模块将安全规则和用户历史数据发送给安全模块。

[161]步骤 711: 安全模块进行风险识别,确定采用的校验方式。本流程中确定采用密码结合数字证书校验方式。

[162]步骤 713: 安全模块向存储模块请求密码和数字证书信息。

[163]步骤 715: 存储模块依据用户标识等提取该用户的第一密码信息和第一数字证书信息,并发送给安全模块。

[164]步骤 717: 安全模块将采用密码结合数字证书校验方式的信息、第一密码信息和第一数字证书信息发送给验证执行模块。

[165]步骤 719: 验证执行模块向第一客户端发送密码结合数字证书校验消息,该消息中包含密码类型信息。

[166]第一客户端接收到密码结合数字证书校验消息后,一方面会向用户展现要求用户输入上述类型密码的界面。例如要求用户输入指纹、人脸、PIN 密码等作为第二密码信息。另一方面,调用本地已安装的数字证书的信息作为第二数字证书信息。

[167]步骤 721: 第一客户端获取用户输入的第二密码信息以及本地的第二数字证书信息,并发送给验证执行模块。

[168]步骤 723: 验证执行模块利用第一密码信息、第二密码信息、第一数字证书信息和第二数字证书信息进行校验。

[169]必须密码信息和数字证书都通过校验才认为校验通过。

[170]步骤 725: 校验成功后,触发支付逻辑。

[171]图 8 出了根据一个实施例的在支付流程中采用跳转至第三方信息码客户端的流程图,如图 8 中所示,该流程可以包括以下步骤。

[172]步骤 801: 第二客户端扫描第一客户端的第三方信息码。

[173]步骤 803: 第二客户端向信息码服务器端的验证执行模块发送码支付请求。

[174]步骤 805: 验证执行模块向安全模块进行风险咨询。

[175]步骤 807: 安全模块向存储模块发送安全规则和用户历史数据的查询。

[176]步骤 809: 存储模块将安全规则和发送给安全模块。

[177]步骤 811: 安全模块进行风险识别, 确定跳转至第三方信息码对应的客户端。

[178]例如用户历史数据为用户设置的支付限额, 而本次支付金额超过该支付限额, 因此跳转至第三方信息码对应的客户端。

[179]步骤 813: 安全模块将校验方式的信息发送给验证执行模块。

[180]步骤 815: 验证执行模块向第一客户端发送指示跳转至第三方信息码对应客户端的链接。

[181]步骤 817: 用户点击该链接后, 由第一客户端跳转至第三方信息码对应的客户端。

[182]步骤 819: 第三方信息码对应的客户端向验证执行模块发送支付请求, 以由验证执行模块触发支付逻辑。

[183]由以上各实施例可以看出, 本发明能够采用不同的校验方式对用户身份进行核验, 保障用户体验的前提下尽可能提高安全性。

[184]上述对本说明书特定实施例进行了描述。其它实施例在所附权利要求书的范围内。在一些情况下, 在权利要求书中记载的动作或步骤可以按照不同于实施例中的顺序来执行并且仍然可以实现期望的结果。另外, 在附图中描绘的过程不一定要求示出的特定顺序或者连续顺序才能实现期望的结果。在某些实施方式中, 多任务处理和并行处理也是可以的或者可能是有利的。

[185]图 9 示出了根据一个实施例的信息处理装置的示意性框图。该装置设置于信息码服务器端, 如图 9 所示, 该装置 900 包括: 接收单元 910、识别单元 920、执行单元 930 和发送单元 940。其中各组成单元的主要功能如下。

[186]接收单元 910, 被配置为接收来自第二客户端的信息码处理请求, 信息码处理请求由第二客户端扫描第一客户端嵌入的第三方信息码后发送。

[187]识别单元 920, 被配置为依据信息码处理请求进行风险识别。

[188]执行单元 930, 被配置为依据识别得到的风险信息和预设的安全规则, 执行相应的处理逻辑。

[189]发送单元 940, 被配置为向第一客户端发送处理逻辑的处理结果。

[190]作为其中一种实现方式, 上述识别单元 920, 具体被配置为: 依据信息码处理请求携带的交易信息、设备信息、环境信息和时间信息中的至少一种, 识别得到风险信息; 或者, 依据信息码处理请求携带的用户信息查询用户的历史数据, 依据用户的历史数据识别得到风险信息。

[191]作为其中一种实现方式, 执行单元 930 可以包括: 确认子单元 931、校验子单元 932 和执行子单元 933。

[192]确认子单元 931, 被配置为依据识别得到的风险信息查询预设的安全规则, 确定是

否执行安全校验。

[193]校验子单元 932, 被配置为若确认子单元 931 确定执行安全校验, 则执行与风险信息对应的安全校验。

[194]执行子单元 933, 被配置为若通过安全校验, 则执行信息码对应的处理逻辑; 若确认子单元 931 确定不执行安全校验, 则执行信息码对应的处理逻辑。

[195]其中, 安全校验可以包括但不限于: 用户确认、密码校验、数字证书校验、密码结合数字证书校验或者跳转至第三方信息码对应的客户端。

[196]作为一种优选的实施方式, 校验子单元 932 在执行密码校验时, 具体被配置为: 依据信息码处理请求携带的用户信息, 确定用户最新设置的密码类型信息和第一密码信息; 向第一客户端发送包含密码类型信息的密码校验消息; 获取第一客户端发送的第二密码信息, 利用第二密码信息和第一密码信息进行校验。

[197]作为另一种优选的实施方式, 校验子单元 932 在执行数字证书校验时, 具体被配置为: 依据信息码处理请求携带的用户信息, 确定与用户信息对应的第一数字证书信息; 向第一客户端发送校验数字证书的消息; 获取第一客户端发送的第二数字证书信息, 利用第二数字证书信息和第一数字证书信息进行校验。

[198]作为再一种优选的实施方式, 校验子单元 932 在执行密码结合数字证书校验时, 具体被配置为: 依据信息码处理请求携带的用户信息, 确定与用户信息对应的密码类型信息、第一密码信息和第一数字证书信息; 向第一客户端发送校验密码和数字证书的消息; 获取第一客户端发送的第二密码信息和第二数字证书信息, 利用第一密码信息、第二密码信息、第一数字证书信息和第二数字证书信息进行校验。

[199]需要说明的是, 上述装置中的各单元和子单元可以设置于一个设备或模块中实现, 也可以设置于多个设备或模块中实现。例如, 上述接收单元 910、发送单元 940、校验子单元 932 和执行子单元 933 可以设置于图 4 至图 8 所示实施例中的验证执行模块中。上述识别单元 920 和确认子单元 931 可以设置于图 4 至图 8 所示实施例中的安全模块中。

[200]图 10 示出根据另一个实施例的信息处理装置的示意性框图。该装置设置于第一客户端, 如图 10 所示, 该装置 1000 包括: 展现单元 1001 和交互单元 1002。其中各组成单元的主要功能如下。

[201]展现单元 1001, 被配置为响应于打开第三方信息码的触发事件, 展现包含第三方信息码的界面, 以便于第二客户端扫描第三方信息码并触发第三方信息码的处理逻辑。

[202]交互单元 1002, 被配置为获取处理逻辑的处理结果。

[203]展现单元 1001, 还被配置为展现包含处理结果的界面。

[204]其中, 打开第三方信息码的触发事件可以包括: 用户触发第一客户端中打开第三方信息码的组件; 或者, 用户在锁屏界面上执行的预设手势操作。

[205]作为可实现的方式,展现单元 1001 在展现包含处理结果的界面时,具体被配置为:从当前界面跳转至包含处理结果的界面;或者,以通知消息的方式展现包含处理结果的界面。

[206]更进一步地,交互单元 1002 可以被配置为:接收信息码服务器端发送的包含密码类型信息的密码校验消息,将用户输入的第二密码信息发送给信息码服务器端;或者接收信息码服务器端发送的校验数字证书的消息,向信息码服务器端发送第二数字证书信息;或者,接收信息码服务器端发送的校验密码和数字证书的消息,该消息包含密码类型信息,向信息码服务器端发送第二数字证书信息。

[207]展现单元 1001 进一步被配置为:在交互单元 1002 接收到包含密码类型信息的密码校验消息以及校验密码和数字证书的消息后,展示输入对应类型密码的提示界面。

[208]根据另一方面的实施例,还提供一种计算机可读存储介质,其上存储有计算机程序,当所述计算机程序在计算机中执行时,令计算机执行图 1 或图 3 所描述的方法。

[209]根据再一方面的实施例,还提供一种计算设备,包括存储器和处理器,所述存储器中存储有可执行代码,所述处理器执行所述可执行代码时,实现图 1 或图 3 所述的方法。

[210]本说明书中的各个实施例均采用递进的方式描述,各个实施例之间相同相似的部分互相参见即可,每个实施例重点说明的都是与其他实施例的不同之处。尤其,对于装置实施例而言,由于其基本相似于方法实施例,所以描述的比较简单,相关之处参见方法实施例的部分说明即可。

[211]本领域技术人员应该可以意识到,在上述一个或多个示例中,本发明所描述的功能可以用硬件、软件、固件或它们的任意组合来实现。当使用软件实现时,可以将这些功能存储在计算机可读介质中或者作为计算机可读介质上的一个或多个指令或代码进行传输。

[212]以上所述的具体实施方式,对本发明的目的、技术方案和有益效果进行了进一步详细说明,所应理解的是,以上所述仅为本发明的具体实施方式而已,并不用于限定本发明的保护范围,凡在本发明的技术方案的基础之上,所做的任何修改、等同替换、改进等,均应包括在本发明的保护范围之内。

权利要求书

1、信息处理方法，由信息码服务器端执行，包括：

接收来自第二客户端的信息码处理请求，所述信息码处理请求由所述第二客户端扫描第一客户端嵌入的第三方信息码后发送；

依据所述信息码处理请求进行风险识别；

依据识别得到的风险信息和预设的安全规则，执行相应的处理逻辑；

向所述第一客户端发送所述处理逻辑的处理结果。

2、根据权利要求1所述的方法，其中，所述依据所述信息码处理请求进行风险识别包括：

依据所述信息码处理请求携带的交易信息、设备信息、环境信息和时间信息中的至少一种，识别得到风险信息；或者，

依据所述信息码处理请求携带的用户信息查询所述用户的历史数据，依据所述用户的历史数据识别得到风险信息。

3、根据权利要求1所述的方法，其中，所述依据识别得到的风险信息和预设的安全规则，执行相应的处理逻辑包括：

依据识别得到的风险信息查询预设的安全规则，确定是否执行安全校验；

如果是，执行与所述风险信息对应的安全校验后，执行所述信息码对应的处理逻辑；

否则，执行信息码对应的处理逻辑。

4、根据权利要求3所述的方法，其中，所述安全校验包括：

用户确认、密码校验、数字证书校验、密码结合数字证书校验或者跳转至第三方信息码对应的客户端。

5、根据权利要求4所述的方法，其中，所述密码校验包括：

依据所述信息码处理请求携带的用户信息，确定用户最新设置的密码类型信息和第一密码信息；

向所述第一客户端发送包含所述密码类型信息的密码校验消息；

获取所述第一客户端发送的第二密码信息，利用所述第二密码信息和第一密码信息进行校验。

6、根据权利要求4所述的方法，其中，所述数字证书校验包括：

依据所述信息码处理请求携带的用户信息，确定与所述用户信息对应的第一数字证书信息；

向所述第一客户端发送校验数字证书的消息；

获取所述第一客户端发送的第二数字证书信息，利用所述第二数字证书信息和所述第一数字证书信息进行校验。

7、根据权利要求4所述的方法，其中，所述密码结合数字证书校验包括：

依据所述信息码处理请求携带的用户信息，确定与所述用户信息对应的密码类型信息、第一密码信息和第一数字证书信息；

向所述第一客户端发送校验密码和数字证书的消息；

获取所述第一客户端发送的第二密码信息和第二数字证书信息，利用第一密码信息、第二密码信息、第一数字证书信息和第二数字证书信息进行校验。

8、根据权利要求1至7中任一项所述的方法，其中，所述信息码包括支付码，所述处理逻辑包括支付处理。

9、信息处理方法，由第一客户端执行，包括：

响应于打开第三方信息码的触发事件，展现包含第三方信息码的界面，以便于第二客户端扫描所述第三方信息码并触发所述第三方信息码的处理逻辑；

获取到信息码服务器端发送的所述处理逻辑的处理结果后，展现包含所述处理结果的界面。

10、根据权利要求9所述的方法，其中，所述打开第三方信息码的触发事件包括：

用户触发所述第一客户端中打开第三方信息码的组件；或者，

用户在锁屏界面上执行的预设手势操作。

11、根据权利要求9或10所述的方法，还包括：

接收到所述信息码服务器端发送的包含密码类型信息的密码校验消息后，展示输入所述类型密码的提示界面，将用户输入的第二密码信息发送给所述信息码服务器端；或者，

接收到所述信息码服务器端发送的校验数字证书的消息后，向所述信息码服务器端发送第二数字证书信息；或者，

接收到所述信息码服务器端发送的校验密码和数字证书的消息后，该消息包含密码类型信息，展示输入所述类型密码的提示界面，并将第二数字证书信息以及用户输入的第二密码信息发送给信息码服务器端。

12、信息处理装置，设置于信息码服务器端，该装置包括：

接收单元，被配置为接收来自第二客户端的信息码处理请求，所述信息码处理请求由所述第二客户端扫描第一客户端嵌入的第三方信息码后发送；

识别单元，被配置为依据所述信息码处理请求进行风险识别；

执行单元，被配置为依据识别得到的风险信息 and 预设的安全规则，执行相应的处理逻辑；

发送单元，被配置为向所述第一客户端发送所述处理逻辑的处理结果。

13、根据权利要求12所述的装置，其中，所述识别单元，具体被配置为：

依据所述信息码处理请求携带的交易信息、设备信息、环境信息和时间信息中的至少一种，识别得到风险信息；或者，

依据所述信息码处理请求携带的用户信息查询所述用户的历史数据，依据所述用户的历史数据识别得到风险信息。

14、根据权利要求 12 所述的装置，其中，所述执行单元包括：

确认子单元，被配置为依据识别得到的风险信息查询预设的安全规则，确定是否执行安全校验；

校验子单元，被配置为若所述确认子单元确定执行安全校验，则执行与所述风险信息对应的安全校验；

执行子单元，被配置为若通过安全校验，则执行所述信息码对应的处理逻辑；若所述确认子单元确定不执行安全校验，则执行所述信息码对应的处理逻辑。

15、根据权利要求 14 所述的装置，其中，所述安全校验包括：

用户确认、密码校验、数字证书校验、密码结合数字证书校验或者跳转至第三方信息码对应的客户端。

16、根据权利要求 15 所述的装置，其中，所述校验子单元在执行密码校验时，具体被配置为：依据所述信息码处理请求携带的用户信息，确定用户最新设置的密码类型信息和第一密码信息；向所述第一客户端发送包含所述密码类型信息的密码校验消息；获取所述第一客户端发送的第二密码信息，利用所述第二密码信息和第一密码信息进行校验。

17、根据权利要求 15 所述的装置，其中，所述校验子单元在执行数字证书校验时，具体被配置为：依据所述信息码处理请求携带的用户信息，确定与所述用户信息对应的第一数字证书信息；向所述第一客户端发送校验数字证书的消息；获取所述第一客户端发送的第二数字证书信息，利用所述第二数字证书信息和所述第一数字证书信息进行校验。

18、根据权利要求 15 所述的装置，其中，所述校验子单元在执行密码结合数字证书校验时，具体被配置为：依据所述信息码处理请求携带的用户信息，确定与所述用户信息对应的密码类型信息、第一密码信息和第一数字证书信息；向所述第一客户端发送校验密码和数字证书的消息；获取所述第一客户端发送的第二密码信息和第二数字证书信息，利用第一密码信息、第二密码信息、第一数字证书信息和第二数字证书信息进行校验。

19、根据权利要求 12 至 18 中任一项所述的装置，其中，所述信息码包括支付码，所述处理逻辑包括支付处理。

20、信息处理装置，设置于第一客户端，该装置包括：

展现单元，被配置为响应于打开第三方信息码的触发事件，展现包含第三方信息码的界面，以便于第二客户端扫描所述第三方信息码并触发所述第三方信息码的处理逻辑；

交互单元，被配置为获取信息码服务器端发送的所述处理逻辑的处理结果；

所述展现单元，还被配置为展现包含所述处理结果的界面。

21、根据权利要求 20 所述的装置，其中，所述打开第三方信息码的触发事件包括：

用户触发所述第一客户端中打开第三方信息码的组件；或者，

用户在锁屏界面上执行的预设手势操作。

22、根据权利要求 20 或 21 中任一项所述的装置，其中，所述交互单元进一步被配置为：接收所述信息码服务器端发送的包含密码类型信息的密码校验消息，将用户输入的第二密码信息发送给所述信息码服务器端；或者接收所述信息码服务器端发送的校验数字证书的消息，向所述信息码服务器端发送第二数字证书信息；或者，接收所述信息码服务器端发送的校验密码和数字证书的消息，向所述信息码服务器端发送第二数字证书信息；

所述展现单元进一步被配置为：展示输入所述类型密码的提示界面。

23、一种计算设备，包括存储器和处理器，所述存储器中存储有可执行代码，所述处理器执行所述可执行代码时，实现权利要求 1-11 中任一项所述的方法。